Health Care Policy

The Long Arm of HIPAA: Extending Privacy Regulations to Business Associates

BY JAY NAWROCKI

If your organization is like most, it likely has dozens, if not hundreds, of outside business associates on whom you rely for support in just about every facet of your institution, from direct patient care to administrative operations and facilities management. And it has not been uncommon in the past for some of these vendors, such as independent labs, information technology vendors, or legal and accounting firms, to have access to patient information.

Ideally, these business associates have used this privileged information only as needed to carry out their contracted services. However, no formal agreement stipulating this has been typically required.

That's about to change drastically. Under the Health Insurance Portability and Accountability Act (HIPAA), health care organizations and insurers that provide medical data cannot give information identifying an individual to another business unless a contract is in place that clearly describes how the privacy of that medical data will be protected. Organizations will have until April 14, 2003, to prepare these contracts.

Federal regulations describe in detail what each contract must contain and the steps health care organizations must take to prevent business associates from violating federal law.

Contract Requirements: Say it Right and in Writing

Contracts between health care organizations and business associates must establish how patient data will be used and disclosed. The Centers for Medicare and Medicaid Services (CMS), formerly known as the Health Care Finance Administration, have stated, however, that they won't require that each use and disclosure of lawfully used health information be listed in the contract. Rather, the contract must first state the purpose for which the business associate may use and disclose individually identifiable health information and then indicate the overall reasons and types of people to whom the business associate may make further disclosures.

The business associate's contract also must include provisions that:

- Specifically prohibit the use or further disclosure of information other than what is permitted by the contract
- Define appropriate safeguards that the business associate must put in place to prevent information from being released improperly

- Require the business associate to report to the provider any use or disclosure of medical data that is not stipulated in the contract
- Require the business associate's subcontractors to abide by the same terms as the business associate
- Allow for amendments to medical data to be incorporated into the medical record
- Provide an accounting of all medical data disclosures to the provider of that medical data
- Make available to the Secretary of the Department of Health and Human Services the internal practices and financial accounts related to the use and disclosure of individually identifiable health information for the purpose of conducting a privacy regulation compliance audit.
- Make protected health data available in accordance with federal law
- Authorize the provider to terminate the contract if it finds that the business associate has violated a material term of the contract

One sticking point that may prove difficult for health care organizations is the requirement that contracts also must stipulate that all medical data, if feasible, be returned to the provider or destroyed by the business associate when they are finished with them. If destroying the data is not feasible because they must be retained for specific reasons, such as future audits, the protections in the contract must be extended for as long as the business associate retains the information.

Liability: Watch Your Vendors

While health care organizations won't have to monitor their business associates' compliance with privacy regulations continually, they will be expected to investigate their activities if they receive complaints or believe that a contract violation has occurred.

A health care organization will be in violation of federal law if it is aware of an activity pattern or a business associate's practice that constitutes a material breach or violation of its contract and does not take reasonable steps to rectify the matter or terminate its relationship with that associate.

The penalty for not acting can range from slight--not more than $100 per person per violation--to significant--a fine of not more than $250,000 and/or imprisonment of not more than 10 years if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm.

Exceptions: Some Relief from the Rules

Like most rules, there are exceptions to the business associate contract requirement. For example, the requirement only applies when identifiable patient information is shared. Therefore, if it is possible to strip the identifiable information from the medical data before it is shared, no contract is required. However, doing so could prove difficult as this identifiable information includes the individual's name, contact information, medical records number, health plan beneficiary numbers, account numbers, certificate or license numbers, vehicle identifiers such as license plate numbers, full-face images, and a host of other potential information that could divulge the individual's identity. In addition, the

data must be prepared so that no one with knowledge of or experience with statistical methods could identify an individual from the medical data provided.

Other instances in which business associate agreements are not required include:

- Relationships between a parent organization and its subsidiaries. However, in these instances, certain safeguards must be put in place to ensure that individually identifiable medical data are not accessible by the non-health care component of the business. For example, employees of the non-health care division should not have access to computers or other data storage areas of the subsidiary.
- Relationships between multiple affiliated entities. Organizations that have several health care companies, such as a hospital system or network, may only need one contract with a third-party business if all of the organization's entities are "affiliated entities." This means that each entity's policies must be significantly influenced by the same controlling corporation, and the affiliated entity must document its affiliation.
- Relationships between a health care organization and a financial institution acting on its behalf. This only applies to financial institutions that conduct their transactions by debit, credit, or other payment card; that clear checks; that initiate or process electronic funds transfers; or that conduct any other activity that provides payment for health care services.

Prepare Now

While the provision for business associate agreements is just one aspect of HIPAA, it has significant administrative ramifications. For many organizations, the biggest challenge will be setting up the processes and procedures needed to administer these business associate contracts. It will require health care providers to clearly identify and define the relationships they have with each of their many vendors across every aspect of their organization's operations--and they must be able to continue to capture this information as old vendors leave and new ones come on board. Procedures are also required for tracking vendor compliance, investigating complaints, and dealing with exceptions to the rules.

With just 18 months left until the business associate regulations go into effect, most health care organizations will have their work cut out for them in developing effective procedures.

Jay Nawrocki is a health care policy analyst with CCH, Inc., Riverwoods, Ill., a provider of health law information, services, and compliance e-learning. He can be reached at (847) 267-7000.

This article first appeared in the September 2001 issue of Trustee

"Trustee" is published by Health Forum, Inc. an American Hospital Association information company.